

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2002-196982
(P2002-196982A)

(43)公開日 平成14年7月12日(2002.7.12)

(51)IntCl ⁷	識別記号	F I	テ-リ-ト(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 1 1 B 20/10		G 1 1 B 20/10	H 5 C 0 5 3
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 C 5 D 0 4 4
9/32			6 7 5 A 5 J 1 0 4
H 0 4 N 5/91		H 0 4 N 5/91	P

審査請求 未請求 請求項の数8 OL (全 20 頁) 最終頁に続く

(21)出願番号 特願2000-395722(P2000-395722)

(22)出願日 平成12年12月26日(2000.12.26)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 加藤 拓

東京都府中市東芝町1番地 株式会社東芝
府中事業所内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B017 AA01 AA06 BA07 CA09

5C053 FA13 FA25 JA21 KA01 LA15

5D044 BC04 CC04 DE17 DE50 EF05

FG18 JJ01

5J104 AA07 AA12 AA15 AA16 EA06

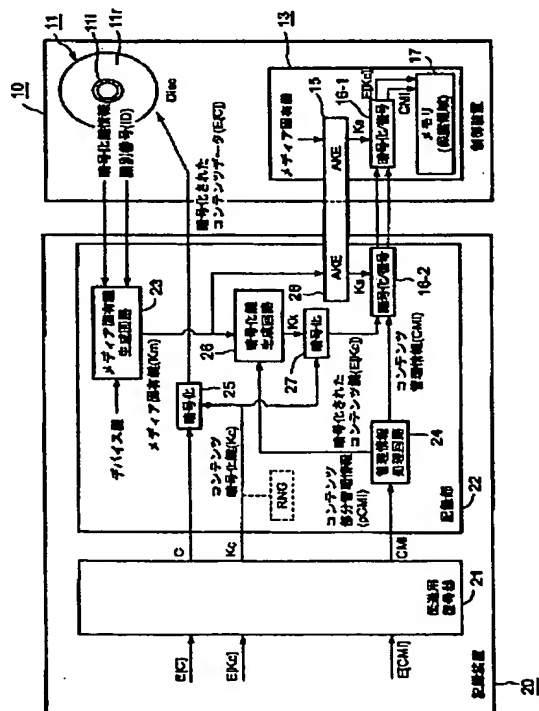
EA17 KA02 KA04 NA02 PA14

(54)【発明の名称】 情報記録媒体、記録/再生装置及び方法

(57)【要約】

【課題】 コンテンツデータを記録しつつ、不正な利用から保護する。

【解決手段】 著作権付コンテンツデータが再生可能に暗号化されて記録される媒体部(11)と、著作権付コンテンツデータの記録/再生処理の可否を制御するための管理情報が記録され、且つ記録処理を行なう記録装置(20)及び再生処理を行なう再生装置の各々に対する認証機能を有する制御装置(13)とを備えた情報記録媒体(10)を用いる。これにより、認証機能により認証され、且つ管理情報により記録/再生可能とされたときのみ、コンテンツデータを記録/再生できる。



【特許請求の範囲】

【請求項1】 著作権付コンテンツデータが暗号化されて記録される媒体部と、

前記著作権付コンテンツデータの記録／再生処理の可否を制御するための管理情報が記録され、且つ前記記録処理を行なう記録装置及び前記再生処理を行なう再生装置の各々に対する認証機能を有する制御装置と、を備えたことを特徴とする情報記録媒体。

【請求項2】 請求項1に記載の情報記録媒体において、

前記制御装置は、前記媒体部から読み出された識別情報から前記記録装置又は前記再生装置が作成した記録媒体固有鍵に基づいて、前記認証機能を実行することを特徴とする情報記録媒体。

【請求項3】 請求項1又は請求項2に記載の情報記録媒体において、

前記媒体部を収容するための媒体保護手段を備えており、

前記制御装置は、前記媒体保護手段に取付けられたことを特徴とする情報記録媒体。

【請求項4】 請求項1乃至請求項3のいずれか1項に記載の情報記録媒体において、

前記媒体部と前記制御装置とは、互いに離間して設けられたことを特徴とする情報記録媒体。

【請求項5】 著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる記録装置であって、

記録対象の著作権付コンテンツデータと共に与えられる管理情報に基づいて、前記媒体部への記録処理の可否を判定する管理情報処理手段と、

前記管理情報処理手段による判定結果が記録可のとき、前記著作権付コンテンツデータを暗号化して前記媒体部に記録するコンテンツ記録手段と、

前記管理情報処理手段による判定結果が記録可のとき、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記管理情報を前記制御装置に転送する管理情報転送手段と、

を備えたことを特徴とする記録装置。

【請求項6】 著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる再生装置であって、

前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記制御装置から管理情報を読み出す管理情報読出手段と、

前記管理情報読出手段により読み出された管理情報に基づいて、前記再生処理の可否を判定する管理情報処理手段と、

前記管理情報処理手段による判定結果が再生可のとき、

前記媒体部内の暗号化された著作権付コンテンツデータを復号して再生するコンテンツ復号手段と、を備えたことを特徴とする再生装置。

【請求項7】 著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる記録方法であって、

記録対象の著作権付コンテンツデータと共に与えられる管理情報に基づいて、前記媒体部への記録処理の可否を判定する管理情報処理ステップと、

前記管理情報処理ステップによる判定結果が記録可のとき、前記著作権付コンテンツデータを暗号化して前記媒体部に記録するコンテンツ記録ステップと、

前記管理情報処理ステップによる判定結果が記録可のとき、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記管理情報を前記制御装置に転送する管理情報転送ステップと、を含んでいることを特徴とする記録方法。

【請求項8】 著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる再生方法であって、

前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記制御装置から管理情報を読み出す管理情報読出ステップと、

前記管理情報読出ステップにより読み出された管理情報に基づいて、前記再生処理の可否を判定する管理情報処理ステップと、

前記管理情報処理ステップによる判定結果が再生可のとき、前記媒体部内の暗号化された著作権付コンテンツデータを復号して再生するコンテンツ復号ステップと、を含んでいることを特徴とする再生方法。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 本発明は、著作権付コンテンツデータを記録可能で、且つ不正な利用から保護し得る情報記録媒体、記録／再生装置及び方法に関する。

【0002】

【従来の技術】 近年、著作権付コンテンツデータ等の情報を記録する分野では、DVD等の如き、読取り専用領域及び書込可能領域といった単純な記録領域のみからなる情報記録媒体が広く知られている。

【0003】 ここで、著作権付コンテンツデータは、読取専用領域に事前に記録される場合、不正な記録装置を用いた不正な書換えから保護される。

【0004】

【発明が解決しようとする課題】 しかしながら以上のような情報記録媒体では、読取専用領域を用いるため、正当な記録装置を用いた正当な記録が実行できないことになる。一方、著作権付コンテンツデータが書込可能領域

に記録される場合、不正な記録装置を用いた不正な書換え等の利用（例、改ざん後の利用等）が可能となってしまう。

【0005】すなわち、著作権付コンテンツデータを不正な利用から保護しつつ、正当な記録も可能な情報記録媒体が存在しない問題がある。

【0006】本発明は上記実情を考慮してなされたもので、コンテンツデータを記録可能で、且つ不正な利用から保護し得る情報記憶媒体、記録／再生装置及び方法を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明の骨子は、情報記録媒体のコンテンツ記録領域とは切り離された場所に制御装置を備えた構成により、単純な情報記録媒体の手軽さを維持しつつ、複雑なセキュリティ機能を実現する。

【0008】具体的には、所定の情報記録媒体本体と、対応する制御装置との組合せのときのみ、情報記憶媒体内のコンテンツデータを利用できる構成により、レベルの高いセキュリティ機能を実現する。

【0009】ここで、セキュリティ機能としては、例えば、コンテンツのコピー枚数制御、コンテンツのチェックイン／チェックアウト機能（<http://www.Sdmi.org/>，“SDMI Portable Device Specification Part 1, Version 1.0”参照）など多様なコンテンツ保護機能などがある。

【0010】さて以上のような本発明の骨子に基づき、具体的には以下のような手段が講じられる。

【0011】第1の発明は、著作権付コンテンツデータが暗号化されて記録される媒体部と、前記著作権付コンテンツデータの記録／再生処理の可否を制御するための管理情報が記録され、且つ前記記録処理を行なう記録装置及び前記再生処理を行なう再生装置の各々に対する認証機能を有する制御装置と、を備えた情報記録媒体である。

【0012】これにより、認証機能により認証され、且つ管理情報により記録／再生可能とされたときのみ、コンテンツデータを記録／再生できる情報記録媒体が実現されるため、コンテンツデータを記録可能で、且つ不正な利用から保護することができる。

【0013】第2の発明は、第1の発明において、前記制御装置としては、前記媒体部から読み出された識別情報から前記記録装置又は前記再生装置が作成した記録媒体固有鍵（以下、メディア固有鍵という）に基づいて、前記認証機能を実行する情報記録媒体である。

【0014】これにより、媒体部と制御装置との組合せが一致しないと制御装置が相手装置（記録／再生装置）を認証しないので、第1の発明の作用に加え、制御装置又は媒体部の付替えといった改造による不正を阻止することができる。

【0015】第3の発明は、第1又は第2の発明におい

て、前記媒体部を収容するための媒体保護手段を備えており、前記制御装置としては、前記媒体保護手段に取付けられた情報記録媒体である。

【0016】これにより、第1又は第2の発明が簡易な構成で実現できるので、第1又は第2の発明の作用を奏する情報記録媒体を容易且つ確実に製造することができる。

【0017】第4の発明は、第1～第3のいずれかの発明において、前記媒体部と前記制御装置とは、互いに離間して設けられた情報記録媒体である。

【0018】これにより、第1～第3の発明を、固定的に設けられた制御装置と、回転可能な媒体部（例、ディスク、テープ等）という構成により容易に実現できる。

【0019】第5の発明は、著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる記録装置であって、記録対象の著作権付コンテンツデータと共に与えられる管理情報に基づいて、前記媒体部への記録処理の可否を判定する管理情報処理手段と、前記管理情報処理手段による判定結果が記録可のとき、前記著作権付コンテンツデータを暗号化して前記媒体部に記録するコンテンツ記録手段と、前記管理情報処理手段による判定結果が記録可のとき、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記管理情報を前記制御装置に転送する管理情報転送手段と、を備えた記録装置である。なお、第5の発明は、同様の技術内容をもつ記録方法として表現してもよい。

【0020】これにより、第1の発明の作用に加え、認証機能により認証され、且つ管理情報により記録可能とされたときのみ、コンテンツデータを記録するため、コンテンツデータを不正な利用から保護することができる。

【0021】第6の発明は、著作権付コンテンツデータが暗号化されて記録される媒体部と、前記媒体部に対する記録／再生処理の可否を制御するための制御装置とを備えた情報記録媒体を用いる再生装置であって、前記制御装置との間で認証処理を行ない、認証結果が可のとき、前記制御装置から管理情報を読み出す管理情報読出手段と、前記管理情報読出手段により読み出された管理情報に基づいて、前記再生処理の可否を判定する管理情報処理手段と、前記管理情報処理手段による判定結果が再生可のとき、前記媒体部内の暗号化された著作権付コンテンツデータを復号して再生するコンテンツ復号手段と、を備えた再生装置である。なお、第6の発明は、同様の技術内容をもつ再生方法として表現してもよい。

【0022】これにより、第1の発明の作用に加え、認証機能により認証され、且つ管理情報により再生可能とされたときのみ、コンテンツデータを再生するため、コンテンツデータを不正な利用から保護することができ

る。

【0023】

【発明の実施の形態】以下、本発明の各実施形態について図面を参照して説明する。

(第1の実施形態) 図1及び図2は本発明の第1の実施形態に係る情報記録媒体の構成を示す模式図であり、図3はこの情報記録媒体及び記録装置の構成を示す模式図であり、図4はこの情報記録媒体及び再生装置の構成を示す模式図である。

【0024】ここで、情報記録媒体10は、図1に示すように、DVD-RAMディスク(記録用の媒体)11と、このDVD-RAMディスク11を回転可能に収容する略正方形の保護ケース12と、この保護ケース12の一隅に取付けられた制御装置13とを備えている。なお、情報記録媒体10は、保護ケース12の内部に制御装置13を備えた構成に限らず、保護ケース12の外部に制御装置13を取付けた構成としてもよい。

【0025】DVD-RAMディスク11は、記録用の媒体の一例であり、ディスク内周側に位置する読出専用のリードイン(Lead-in)領域11iと、このリードイン領域よりも外周側に位置する読出/書込可能な記録領域11rとを備えている。なお、DVD-RAMディスク11は、記録用の媒体の一例であり、適宜、他種類の記録用の媒体(例、D-VHS等)に変えてもよい。また、他種類の記録用の媒体としては、ディスク状の媒体に限らず、例えばテープ状の媒体を用いてもよい。

【0026】リードイン領域11iは、暗号化された鍵情報及び各々のDVD-RAMディスク11を区別するための識別番号(ID)がディスク製造時に書込まれた読出専用領域である。

【0027】記録領域11rは、暗号化されたコンテンツデータE[C]が読出/書込可能に記録される領域である。なお、コンテンツデータCは、ここでは著作権付きコンテンツを表現するためのデータを意味している。

【0028】保護ケース12は、回転可能にDVD-RAMディスク11を保持し、そのDVD-RAMディスク11の一部を記録時/再生時のみ露出させるためのスライド蓋付窓部14が形成されている。

【0029】制御装置13は、図2に示すように、予め当該DVD-RAMディスク11に対応するメディア固有鍵K_pを秘密に格納しており、且つ認証・鍵交換部15、暗号化/復号回路16-1及びメモリ17を備えている。

【0030】認証・鍵交換部15は、アクセスしてきた記録装置20又は再生装置30の正当性を確認するため、読出/書込の際に、アクセスしてきた装置との間で自装置13内のメディア固有鍵K_pに基づいて、所定の認証及び鍵交換(AKE: Authentication and Key Exchange)処理を行ない、共有鍵K_sを記録装置20や再生装置30と共有するものである。

【0031】なお、制御装置13のメディア固有鍵K_pと、記録装置20及び再生装置30のメディア固有鍵K_mとの関係は、互いに同じ値($K_p = K_m$)としてもよく、又は、互いに違う値($K_p \neq K_m$ 、例、K_pとK_mは公開鍵と秘密鍵の関係)としてもよいが、当該関係に応じて認証・鍵交換部15の処理内容を設定する必要がある。

【0032】暗号化/復号回路16-1は、アクセスしてきた記録装置20又は再生装置30と、自装置13との間の通信路における盗聴や改ざん等の攻撃を防ぐため、認証・鍵交換部15により共有された共有鍵K_sに基づいて、メモリ17内のデータを暗号化して記録装置20又は再生装置30に送出する機能と、記録装置20又は再生装置30から受けた暗号化データを復号して復号結果をメモリ17に記録する機能をもっている。

【0033】次に、記録装置20及び再生装置30の構成について順次説明する。なお、記録装置20と再生装置30を別々に設けた場合について述べるが、これに限らず、記録装置20と再生装置30とを合わせた記録/再生装置として設けてもよい。また、記録装置20及び再生装置30は、従来同様に、自装置13内に秘密に保持されたデバイス鍵と呼ばれる、装置固有の鍵を備えている。

【0034】記録装置20は、図3に示すように、伝送用復号器21及び記録部22を備えている。

【0035】伝送用復号器21は、記録装置20内部から受ける夫々暗号化されたコンテンツデータE[C]、暗号化されたコンテンツ暗号化鍵E[K_c]及び暗号化されたコンテンツ管理情報E[CMI]を復号し、夫々得られたコンテンツデータC、コンテンツ暗号化鍵K_c及びコンテンツ管理情報CMI(Content Management Information)を記録部22に入力する機能をもっている。

【0036】記録部22は、伝送用復号器23から得られたコンテンツデータC、コンテンツ暗号化鍵K_c及びコンテンツ管理情報CMIに基づいて、コンテンツ暗号化鍵K_cにより暗号化して得た暗号化されたコンテンツデータE[C]をDVD-RAMディスク11の記録領域11rに書込む機能と、コンテンツ暗号化鍵K_cを暗号化して得た暗号化されたコンテンツ暗号化鍵E[K_c]、及びコンテンツ管理情報CMIを夫々共有鍵K_sで暗号化して制御装置13に送出する機能をもっている。なお、記録装置20が伝送用復号器21からコンテンツ暗号化鍵K_cを入力しない方式の場合、記録部22は、予め設けられた乱数生成器RNGにより生成した乱数をコンテンツ暗号化鍵K_cとして用いても良い。

【0037】具体的には記録部22は、メディア固有鍵生成回路23、管理情報処理回路24、コンテンツ暗号化部25、暗号化鍵生成回路26、鍵暗号化部27、認証・鍵交換部28、暗号化/復号回路16-2を備えて

いる。

【0038】メディア固有鍵生成回路23は、DVD-RAMディスク11のリードイン領域11iから読み出された暗号化鍵情報及び識別情報IDと、自己のデバイス鍵とに基づいてメディア固有鍵Kmを生成する機能と、このメディア固有鍵Kmを暗号化鍵生成回路25及び認証・鍵交換部28に送出する機能とをもっている。

【0039】ここで、メディア固有鍵Kmは、あるDVD-RAMディスク11に記録されたコンテンツが正当な全ての再生装置30で再生可能となるように、正当な全ての記録装置20において、全て同じ値に生成される。

【0040】管理情報処理回路24は、伝送用復号器21から入力されたコンテンツ管理情報CMIに基づいて記録禁止か否かを判定する機能と、判定結果が記録禁止を示すときには記録処理を終了する機能とをもっている。

【0041】また、管理情報処理回路24は、判定結果が否（記録可能）を示すとき、コンテンツ管理情報CMIからコンテンツ部分管理情報pCMIを抽出する機能と、このコンテンツ部分管理情報pCMIを暗号化鍵生成回路26に送出すると共に、コンテンツ管理情報CMIを暗号化／復号回路16-2に送出する機能とをもっている。

【0042】なお、コンテンツ管理情報CMIは、コンテンツを管理するための情報であり、例えば書誌的事項を管理する内容（例、著作者や著作年月日）、コピー管理に関する内容（例、コピー可能回数）、再生管理に関する内容（例、再生可能回数）等の任意のものが適宜、設定可能である。

【0043】コンテンツ暗号化部25は、伝送用復号器21からのコンテンツ暗号化鍵Kcに基づいて、伝送用復号器21から入力されたコンテンツデータCを暗号化する機能と、得られた暗号化されたコンテンツデータE[C]をDVD-RAMディスク11の記録領域11rに書き込む機能とをもっている。

【0044】暗号化鍵生成回路26は、メディア固有鍵生成回路23から受けたメディア固有鍵Kmと、管理情報処理回路24から受けたコンテンツ部分管理情報pCMIとに基づいて鍵暗号化鍵Kkを生成する機能と、この鍵暗号化鍵Kkを鍵暗号化部に送出する機能とをもっている。

【0045】鍵暗号化部27は、暗号化鍵生成回路26から受けた鍵暗号化鍵Kkを用いてコンテンツ暗号化鍵Kcを暗号化する機能と、得られた暗号化されたコンテンツ鍵E[Kc]を暗号化／復号回路16-2に送出する機能とをもっている。

【0046】認証・鍵交換部28は、メディア固有鍵生成回路23から受けたメディア固有鍵Kmを用いて制御装置13の認証・鍵交換部15との間で認証及び鍵交換

（AKE）処理を行なう機能と、鍵交換処理の結果、制御装置13との間で共有鍵Ksを共有する機能とをもっている。

【0047】暗号化／復号回路16-2は、認証・鍵交換部28により共有された共有鍵Ksに基づいて、鍵暗号化部27から受けた暗号化されたコンテンツ鍵E[Kc]と、管理情報処理回路24から受けたコンテンツ管理情報CMIとの両者を暗号化する機能と、この暗号化により得られた暗号化データを制御装置13に送出する機能とをもっている。なお、記録装置20の暗号化／復号回路16-2は、制御装置13内の暗号化復号回路16-1と基本的に同じ回路であり、後述する再生装置30にも設けられている。すなわち、制御装置13、記録装置20及び再生装置30の各暗号化／復号回路16-1、16-2同士は、基本的に同一構成であり、配置場所が異なるだけである。

【0048】一方、再生装置30は、図4に示すように、伝送用暗号化器31と、再生部32とを備えている。

【0049】伝送用暗号化器31は、再生部32から受けるコンテンツデータC、コンテンツ暗号化鍵Kc及びコンテンツ管理情報CMIの各々を暗号化する機能と、暗号化により得られた暗号化されたコンテンツデータE[C]、暗号化されたコンテンツ鍵E[Kc]及び暗号化されたコンテンツ管理情報E[CMI]を再生装置30の内部に出力する機能とをもっている。

【0050】再生部32は、制御装置13から得られたコンテンツ管理情報CMIに基づいて、再生処理を行なう機能と、再生時には、制御装置13から読み出した暗号化されたコンテンツ鍵E[Kc]を復号してコンテンツ暗号化鍵Kcを得る機能と、DVD-RAMディスク11の記録領域11rから暗号化されたコンテンツデータE[C]を読み出す機能と、読み出した暗号化されたコンテンツデータE[C]をコンテンツ暗号化鍵Kcにより復号する機能と、復号により得たコンテンツデータC及びコンテンツ暗号化鍵Kcを伝送用暗号化部31に出力する機能とをもっている。

【0051】具体的には再生部32は、メディア固有鍵生成回路33、認証・鍵交換部34、暗号化／復号回路16-2、管理情報処理回路36、復号鍵生成回路37、鍵復号部38、コンテンツ復号部39を備えている。

【0052】メディア固有鍵生成回路33は、DVD-RAMディスク11のリードイン領域11iから読み出された暗号化鍵情報及び識別情報IDと、自己のデバイス鍵とに基づいて、メディア固有鍵Kmを生成して暗号化鍵生成回路37及び認証・鍵交換部34に送出する機能をもっている。

【0053】認証・鍵交換部34は、メディア固有鍵生成回路33から受けたメディア固有鍵Kmを用いて制御

装置13の認証・鍵交換部15との間で認証及び鍵交換処理を行なう機能と、制御装置13との間で共有鍵Ksを共有する機能とをもっている。

【0054】暗号化／復号回路16-2は、制御装置13から受けた暗号化データを、認証・鍵交換部34により共有された共有鍵Ksを用いて復号し、得られた暗号化されたコンテンツ鍵E[Kc]を鍵復号部38に送出する一方、得られたコンテンツ管理情報CMIを管理情報処理回路36に送出する機能をもっている。

【0055】管理情報処理回路36は、暗号化／復号回路16-2から受けたコンテンツ管理情報CMIを確認して、再生禁止か否かを判定する機能と、判定結果が再生禁止を示すときには再生処理をせずに終了する機能とをもっている。

【0056】また、管理情報処理回路36は、判定結果が再生可能を示す場合、再生時には、コンテンツ管理情報CMIからコンテンツ部分管理情報pCMIを抽出する機能と、このコンテンツ部分管理情報pCMIを復号鍵生成回路37に送出すると共に、コンテンツ管理情報CMIを伝送用暗号器31に送出する機能と、コンテンツ管理情報CMIに再生可能回数又はコピー可能回数の減少等の所定の処理を施した後、コンテンツ管理情報CMIを暗号化／復号回路16-2に返送する機能とをもっている。

【0057】復号鍵生成回路37は、管理情報処理回路36から受けたコンテンツ部分管理情報pCMIと、メディア固有鍵生成回路33から受けたメディア固有鍵Kmを用いて鍵復号鍵Kkを生成する機能をもっている。

【0058】鍵復号部38は、暗号化／復号回路16-2で復号された暗号化されたコンテンツ鍵E[Kc]を、復号鍵生成回路37により生成された鍵復号鍵Kkに基づいて、復号する機能をもっている。

【0059】コンテンツ復号部39は、DVD-RAMディスク11の記録領域11rから読み出した暗号化されたコンテンツデータE[C]を、鍵復号部38により復号された暗号化されたコンテンツ鍵Kcに基づいて復号する機能と、復号して得たコンテンツデータCを伝送用暗号化器31に出力する機能をもっている。

【0060】次に、以上のように構成された情報記録媒体、記録装置及び再生装置による情報の記録方法及び再生方法について図5及び図6のフローチャートを用いて説明する。なお、コンテンツデータCとしては、著作権付きのものを想定しており、この想定は以下の各実施形態でも同様である。

【0061】(記録方法) 伝送用復号器21は、図3に示すように、記録装置20内部から受ける夫々暗号化されたコンテンツデータE[C]、コンテンツ暗号化鍵E[Kc]及びコンテンツ管理情報E[CMI]を復号し、夫々得られたコンテンツデータC、コンテンツ暗号化鍵Kc及びコンテンツ管理情報CMIを記録部22に

入力する。

【0062】記録部22においては、図3及び図5に示すように、DVD-RAMディスク11のリードイン領域11iから暗号化鍵情報と識別番号IDを讀出すと

(ST1)、メディア固有鍵生成回路23が、これら暗号化鍵情報及び識別情報IDと自己のデバイス鍵とに基づいてメディア固有鍵Kmを生成し、このメディア固有鍵Kmを暗号化鍵生成回路25及び認証・鍵交換部28に送出する。

【0063】一方、記録部22の管理情報処理回路24は、伝送用復号器21から入力されたコンテンツ管理情報CMIを確認して(ST2)、記録禁止か否かを判定し(ST3)、コンテンツ管理情報CMIが記録禁止を示すときには以下の記録処理をせずに終了する。では次に、コンテンツ管理情報CMIが記録可能を示す場合の動作を述べる。

【0064】記録可能の場合、管理情報処理回路24は、コンテンツ管理情報CMIからコンテンツ部分管理情報pCMIを抽出し、このコンテンツ部分管理情報pCMIを暗号化鍵生成回路26に送出すると共に、コンテンツ管理情報CMIを暗号化／復号回路16-2に送出する。

【0065】また一方、コンテンツ暗号化部25は、伝送用復号器21からのコンテンツ暗号化鍵Kcに基づいて、伝送用復号器21から入力されたコンテンツデータCを暗号化し、得られた暗号化されたコンテンツデータE[C]をDVD-RAMディスク11の記録領域11rに書込む(ST4)。

【0066】しかる後、暗号化鍵生成回路26は、コンテンツ部分管理情報pCMI及びメディア固有鍵Kmに基づいて鍵暗号化鍵Kkを生成し、この鍵暗号化鍵Kkを鍵暗号化部27に送出する。

【0067】鍵暗号化部27は、この鍵暗号化鍵Kkを用いてコンテンツ暗号化鍵Kcを暗号化し(ST5)、得られた暗号化されたコンテンツ鍵E[Kc]を暗号化／復号回路16-2に送出する。

【0068】次に、認証・鍵交換部28は、メディア固有鍵Kmを用いて制御装置13の認証・鍵交換部15との間で認証及び鍵交換(AKE)処理を行ない(ST6)、制御装置13との間で共有鍵Ksを共有する。

【0069】暗号化／復号回路16-2は、この共有鍵Ksに基づいて、暗号化されたコンテンツ鍵E[Kc]及びコンテンツ管理情報CMIを暗号化し、得られた暗号化データを制御装置13に送る(ST7)。

【0070】制御装置13は、暗号化／復号回路16-1が、共有鍵Ksに基づいて、この暗号化データを復号し、得られた暗号化されたコンテンツ鍵E[Kc]とコンテンツ管理情報CMIをメモリ17に記録する(ST8)。

【0071】(再生方法) 再生部32においては、図4

及び図6に示すように、DVD-RAMディスク11のリードイン領域11iから暗号化鍵情報と識別番号IDを読出すと(ST11)、メディア固有鍵生成回路33が、これら暗号化鍵情報及び識別情報IDと、自己のデバイス鍵とに基づいて、メディア固有鍵Kmを生成して暗号化鍵生成回路37及び認証・鍵交換部34に送出する。

【0072】次に、認証・鍵交換部34は、メディア固有鍵Kmを用いて制御装置13の認証・鍵交換部15との間で認証及び鍵交換処理を行ない(ST12)、制御装置13との間で共有鍵Ksを共有する。

【0073】制御装置13では、暗号化/復号回路16-1が、メモリ17から読み出した暗号化されたコンテンツ鍵E[Kc]とコンテンツ管理情報CMIを共有鍵Ksにより暗号化し、得られた暗号化データを再生部32に送る(ST13)。

【0074】再生部32では、暗号化/復号回路16-2が、この暗号化データを共有鍵Ksにより復号し、得られた暗号化されたコンテンツ鍵E[Kc]を鍵復号部38に送出する一方、得られたコンテンツ管理情報CMIを管理情報処理回路36に送出する(ST14)。

【0075】管理情報処理回路36は、このコンテンツ管理情報CMIを確認し(ST15)、再生禁止か否かを判定し(ST16)、コンテンツ管理情報CMIが再生禁止を示すときには以下の再生処理をせずに終了する。では次に、コンテンツ管理情報CMIが再生可能を示す場合の動作を述べる。

【0076】再生可能の場合、管理情報処理回路36は、コンテンツ管理情報CMIからコンテンツ部分管理情報pCMIを抽出し、このコンテンツ部分管理情報pCMIを復号鍵生成回路37に送出すると共に、コンテンツ管理情報CMIを伝送用暗号器31に送出する。

【0077】さらに、管理情報処理回路36は、コンテンツ管理情報CMIに再生可能回数又はコピー可能回数の減少等の所定の更新処理を施した後(ST17)、コンテンツ管理情報CMIを暗号化/復号回路16-2により暗号化して制御装置13に送出する。制御装置13は、暗号化されたコンテンツ管理情報CMIを復号してメモリ17に記録する。

【0078】次に、再生部32では、復号鍵生成回路37が、コンテンツ部分管理情報pCMIとステップST11で求めたメディア固有鍵Kmを用いて鍵復号鍵Kkを生成し、この鍵復号鍵Kkを鍵復号部38に送出する。

【0079】鍵復号部38は、この鍵復号鍵Kkに基づいて、暗号化/復号回路16-2で得た暗号化されたコンテンツ鍵E[Kc]を復号し、得られたコンテンツ暗号化鍵Kcをコンテンツ復号部39に送出する(ST18)。なお、これに加え、必要によりコンテンツ暗号化鍵Kcを伝送用暗号化器31に出力してもよい。

【0080】しかる後、再生部32では、コンテンツ復号部39が、DVD-RAMディスク11の記録領域11rから暗号化されたコンテンツデータE[C]を読み出し、この暗号化されたコンテンツデータE[C]をコンテンツ暗号化鍵Kcにより復号し、得られたコンテンツデータCを伝送用暗号化器31に出力する(ST19)。

【0081】伝送用暗号化器31は、このコンテンツデータを再生装置の方式に対応した任意の方式で暗号化し、得られた暗号化されたコンテンツデータE'[C]を出力する。

【0082】上述したように本実施形態によれば、認証機能により認証され、且つ管理情報により記録/再生可能とされたときのみ、コンテンツデータCを記録/再生できる情報記録媒体10、記録装置20及び再生装置30が実現されるため、コンテンツデータを記録可能で、且つ不正な利用から保護することができる。

【0083】すなわち、DVD-RAMディスク11等の如き、情報記録機能のみをもつ単純な記録媒体においても、DVD-RAMディスク11から離して制御装置13を設けるという簡単な拡張により、複雑なセキュリティ機能を実現させることができる。

【0084】例えば、DVD-RAMディスク11の内容をコピーしたとしても、制御装置13のメモリ17内容やメディア固有鍵Kpをコピーできないため、ディスク11のコピーを利用することができず、結果として不正なコピーの頒布を阻止している。

【0085】また、周知のDVD-RAMプレーヤ/レコーダおよびDVD-RAMドライブ等の記録装置20及び再生装置30の形状を一切変更せずに、その内部に、制御装置13の認証、データの暗号化/復号、管理情報の確認といったセキュリティ動作をする回路(記録部22や再生部32等)を追加するだけで、高度なセキュリティ機能を実現することができる。

【0086】また、制御装置13としては、DVD-RAMディスク11から読み出された識別番号ID等から記録装置20又は再生装置30が作成したメディア固有鍵Kmに基づいて、認証処理を実行する構成であり、すなわち、DVD-RAMディスク11と制御装置13との組合せが一致しないと記録/再生装置20、30を認証しないので、制御装置13又はDVD-RAMディスク11の付替えといった改造による不正をも阻止することができる。

【0087】また、制御装置13が保護ケース12に取り付けられた簡易な構成で実現できるので、本発明の情報記録媒体10を容易且つ確実に製造することができる。

【0088】また、DVD-RAMディスク11と制御装置13とは、互いに離間して設けられるので、固定的に設けられた制御装置13と、回転可能な媒体部(例、

ディスク、テープ等)という構成により容易に実現できる。

【0089】(第2の実施形態)図7は本発明の第2の実施形態に係る記録装置及び情報記録媒体の構成を示す模式図であり、図8は同実施形態における再生装置及び情報記録媒体の構成を示す模式図であって、図3及び図4と同一部分には同一符号を付し、異なる部分にはaの添字を付して説明し、ここでは異なる部分について主に述べる。

【0090】すなわち、本実施形態が第1の実施形態と異なる点は、主に、(1)コンテンツ部分管理情報pCMIを利用せず、コンテンツ管理情報CMI内に設けたコピー管理情報CCIを鍵暗号化鍵Kk及び鍵復号鍵Kkの生成に用いる点と、(2)このコピー管理情報CCIをDVD-RAMディスク11の記録領域11rに記録する点と、(3)暗号化されたコンテンツ鍵E[Kc]の記録場所を制御装置13ではなく、DVD-RAMディスク11の記録領域11rとした点と、である。

【0091】これらの変更点に伴い、記録装置20aは、変更された機能ブロックとして、管理情報処理回路24a、暗号鍵生成回路26a及び鍵暗号化部27aを備えている。

【0092】管理情報処理回路24aは、伝送用復号器21から受けたコンテンツ管理情報CMI内のコピー管理情報CCIに基づいて記録禁止か否かを判定する機能と、コピー管理情報CCIが記録禁止を示すときには記録処理をせずに終了する機能とをもっている。

【0093】また、管理情報処理回路24aは、コピー管理情報CCIが記録可能を示す場合、コピー管理情報CCIをDVD-RAMディスク11の記録領域11rに書き込む一方、暗号化鍵生成回路26aに送出する機能をもっている。

【0094】ここで、コピー管理情報CCIは、コンテンツ管理情報CMIのうち、コピー管理に関する部分である。コピー管理情報CCIには、自由にコピー可能な“Copy Freely”、1回だけコピー可能な“Copy One Generation”、それ以上のコピーが禁止される“No More Copies”及び絶対にコピー禁止の“Never Copy”の4つの状態が存在するが、コピー可能であり暗号化等によって、記録媒体上でコンテンツを守る必要がある状態は、“Copy One Generation”のみである。さらに“Copy One Generation”のコンテンツは、1回コピーした後、“No More Copies”の状態に記録される(コピー毎に可能回数が1回減る)。従って、殆どの場合、ここで鍵生成に使われるコピー管理情報はCCI=“No More Copies”である。

【0095】暗号化鍵生成回路26aは、管理情報処理回路24aから受けたコピー管理情報CCIと、前述同様にメディア固有鍵生成回路23から受けたメディア固有鍵Kmとに基づいて、鍵暗号化鍵Kkを生成する機能

と、この鍵暗号化鍵Kkを鍵暗号化部27aに送出する機能とをもっている。

【0096】鍵暗号化部27aは、暗号鍵生成回路26aから受けた鍵暗号化鍵Kkを用いてコンテンツ暗号化鍵Kcを暗号化する前述した機能に加え、得られた暗号化されたコンテンツ鍵E[Kc]を(暗号化/復号回路16-2経由ではなく)DVD-RAMディスク11の記録領域11rに書き込む機能とをもっている。

【0097】一方、再生装置30aは、変更された機能ブロックとして、管理情報処理回路36a、復号鍵生成回路37a及び鍵復号部38aを備えている。

【0098】管理情報処理回路36aは、暗号化/復号回路16-2から受けたコンテンツ管理情報CMIを確認する機能と、コンテンツ管理情報CMIに再生可能回数又はコピー可能回数の減少等の所定の更新処理を施した後、伝送用暗号化器31に出力する機能と、当該コンテンツ管理情報CMIを暗号化/復号回路16-2により暗号化して制御装置13に送出する機能とをもっている。

【0099】復号鍵生成回路37aは、DVD-RAMディスク11から読み出されたコピー管理情報CCIと、前述同様にメディア固有鍵生成回路23から受けたメディア固有鍵Kmとに基づいて鍵復号鍵Kkを生成する機能と、得られた鍵復号鍵Kkを鍵復号部38aに送出する機能とをもっている。

【0100】鍵復号部38aは、DVD-RAMディスク11から読み出された暗号化されたコンテンツ鍵E[Kc]を、復号鍵生成回路37aから受けた鍵復号鍵Kkに基づいて復号する機能と、得られたコンテンツ暗号化鍵Kcをコンテンツ復号部39に送出する機能とをもっている。

【0101】次に、以上のように構成された情報記録媒体、記録装置及び再生装置による情報の記録方法及び再生方法について図9及び図10のフローチャートを用いて説明する。

【0102】(記録方法)図7及び図9に示すように、記録部22aにおいては、前述同様に、ステップST1のID等の読出からメディア固有鍵Kmの生成並びにステップST2のコンテンツ管理情報CMIの確認までを行なう。次に、記録部22aの管理情報処理回路24aは、コンテンツ管理情報CMI内のコピー管理情報CCIに基づいて記録禁止か否かを判定し(ST3a)、コピー管理情報CCIが記録禁止を示すときには以下の記録処理をせずに終了する。では次に、コピー管理情報CCIが記録可能を示す場合の動作を述べる。

【0103】記録可能な場合、コンテンツ暗号化部25は、前述同様に、ステップST4を行ない、暗号化されたコンテンツデータE[C]をDVD-RAMディスク11の記録領域11rに書き込む。

【0104】また、管理情報処理回路24aは、コピー

管理情報CCIをDVD-RAMディスク11の記録領域11rに書込む一方(ST4-2)、暗号化鍵生成回路26に送出する。

【0105】暗号化鍵生成回路26aは、このコピー管理情報CCIとステップST1で得たメディア固有鍵Kmとに基づいて鍵暗号化鍵Kkを生成し、この鍵暗号化鍵Kkを鍵暗号化部27aに送出する。

【0106】鍵暗号化部27aは、この鍵暗号化鍵Kkを用いてコンテンツ暗号化鍵Kcを暗号化し(ST5)、得られた暗号化されたコンテンツ鍵E[Kc]をDVD-RAMディスク11の記録領域11rに書込む(ST5-2)。

【0107】以下前述同様に、記録部22aは、ステップST6の認証及び鍵交換処理を行ない、制御装置13との間で共有鍵Ksを共有する。

【0108】また、暗号化/復号回路16-2は、この共有鍵Ksに基づいて、コンテンツ管理情報CMIを暗号化し、得られた暗号化データを制御装置13に送出(ST7a)。

【0109】制御装置13では、暗号化/復号回路16-1が、共有鍵Ksに基づいて、この暗号化データを復号し、得られたコンテンツ管理情報CMIをメモリ17に記録する(ST8a)。

【0110】(再生方法)図8及び図10に示すように、再生部32aにおいては、前述同様に、ステップST11のID等の読出により、メディア固有鍵Kmの生成を行なう。

【0111】次に、再生部32aは、DVD-RAMディスク11の記録領域11rから暗号化されたコンテンツ鍵E[Kc]とコピー管理情報CCIとを読み出し(ST21)、復号鍵生成回路37aが、このコピー管理情報CCIとメディア固有鍵Kmを用いて鍵復号鍵Kkを生成し、得られた鍵復号鍵Kkを鍵復号部38aに送出する。

【0112】鍵復号部38aは、この鍵復号鍵Kkに基づいて、暗号化されたコンテンツ鍵E[Kc]を復号し、得られたコンテンツ暗号化鍵Kcをコンテンツ復号部39に送出する(ST22)。

【0113】コンテンツ復号部39は、DVD-RAMディスク11から暗号化されたコンテンツデータE[C]を読み出し(ST23)、コンテンツ暗号化鍵Kcを用いて暗号化されたコンテンツデータE[C]を復号し、得られたコンテンツデータCを出力する(ST24)。この時、必要に応じてコンテンツ暗号化鍵Kcもコンテンツ復号部39又は鍵復号部38aから出力される。

【0114】再生部32aでは、ステップST12と同様に認証及び鍵交換(AKE)処理を行ない(ST12)、制御装置13の間で共有鍵Ksを共有する。

【0115】制御装置13は、暗号化/復号回路16-

1が、メモリ17から読み出したコンテンツ管理情報CMIを共有鍵Ksにより暗号化し、得られた暗号化データを再生部32aに送る(ST13a)。

【0116】再生部32aでは、暗号化/復号回路16-2が、この暗号化データを共有鍵Ksにより復号し、得られたコンテンツ管理情報CMIを管理情報処理回路36aに送出する(ST14a)。

【0117】管理情報処理回路36aは、コンテンツ管理情報CMIを確認し(ST15a)、コンテンツ管理情報CMIに再生可能回数又はコピー可能回数の減少等の所定の更新処理を施す(ST17a)。ここでは特に、ステップST15aの確認の際に、コンテンツ管理情報CMIが再生禁止を示したとき、コピー管理情報CCIを変更する(これにより、次の再生時に、復号鍵生成回路37aが鍵復号鍵Kkを正しく生成できないようにし、もって、コンテンツデータCを正しく復号できなくする)。

【0118】しかる後、管理情報処理回路36aは、コンテンツ管理情報CMIを伝送用暗号化器31に出力する一方、当該コンテンツ管理情報CMIを暗号化/復号回路16-2により暗号化して制御装置13に送出する(ST25)。制御装置13は、暗号化されたコンテンツ管理情報CMIを復号してメモリ17に記録する(ST26)。

【0119】上述したように本実施形態によれば、

(1)コンテンツ管理情報CMI内に設けたコピー管理情報CCIを鍵暗号化鍵Kk及び鍵復号鍵Kkの生成に用い、(2)このコピー管理情報CCIをDVD-RAMディスク11の記録領域11rに記録し、(3)暗号化されたコンテンツ鍵E[Kc]の記録場所をDVD-RAMディスク11の記録領域11rとした構成に変形しても、第1の実施形態と同様の効果を得ることができる。

【0120】なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク(フロッピー(登録商標)ディスク、ハードディスクなど)、光ディスク(CD-ROM、DVDなど)、光磁気ディスク(MO)、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【0121】また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0122】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS(オペレーティングシステム)や、データベース管理ソフト、ネットワークソフト等のMW(ミドルウェア)等が本実施形態を実現するための各処理の一部を実行しても良い。

【0123】さらに、本発明における記憶媒体は、コン

ピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0124】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0125】尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0126】また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0127】なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。

【0128】例えば、媒体部は、DVD-RAMディスク11に限らず、任意の記録媒体を使用してもよい。また、記録方法や再生方法は、細かい手順を適宜、前後させてもよい。

【0129】例えば、第1の実施形態の記録方法において、コンテンツ管理情報CMIに基づく記録禁止か否かの判定(ST3)を、暗号化鍵情報及び識別情報IDの読出(ST1)よりも先に行なっても良く、また、暗号化されたコンテンツデータE[C]の書込(ST4)を、暗号化されたコンテンツ鍵E[Kc]及びコンテンツ管理情報CMIの記録(ST8)よりも後に行なっても良い。また、認証及び鍵交換(ST6)を、暗号化されたコンテンツデータE[C]の書込(ST4)よりも先に行ない、認証及び鍵交換(ST6)の結果が良いときのみ、ST4を許可する手順としてもよい。

【0130】いずれにしても、記録禁止か否かの判定(ST3)の後に、暗号化されたコンテンツデータE[C]の書込(ST4)が行われる手順であれば、図3の矢印が上流から下流に向かう範囲で他の手順を適宜、前後させてもよい。

【0131】同様に、第1の実施形態の再生方法において、例えば、コンテンツ管理情報CMIの更新(ST17)を、コンテンツデータCの出力(ST19)よりも後に行なってもよい。

【0132】すなわち、再生禁止か否かの判定(ST16)の後に、コンテンツデータCの出力(ST19)が行われる手順であれば、図4の矢印が上流から下流に向かう範囲で他の手順を適宜、前後させてもよい。

【0133】これらの変形可能な例は第2の実施形態でも同様である。また、各実施形態は可能な限り適宜組み合わせ実施してもよく、その場合、組み合わせられた効

果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0134】その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0135】

【発明の効果】以上説明したように本発明によれば、コンテンツデータを記録可能で、且つ不正な利用から保護することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る情報記録媒体の構成を示す模式図

【図2】同実施形態における情報記録媒体の構成を示す模式図

【図3】同実施形態における情報記録媒体及び記録装置の構成を示す模式図

【図4】同実施形態における情報記録媒体及び再生装置の構成を示す模式図

【図5】同実施形態における記録方法を説明するためのフローチャート

【図6】同実施形態における再生方法を説明するためのフローチャート

【図7】本発明の第2の実施形態に係る記録装置及び情報記録媒体の構成を示す模式図

【図8】同実施形態における再生装置及び情報記録媒体の構成を示す模式図

【図9】同実施形態における記録方法を説明するためのフローチャート

【図10】同実施形態における再生方法を説明するためのフローチャート

【符号の説明】

11…DVD-RAMディスク

11i…リードイン領域

11r…記録領域

12…保護ケース

13…制御装置

14…スライド蓋付窓部

15, 28, 34…認証・鍵交換部

16-1, 16-2…暗号化/復号回路

17…メモリ

20…記録装置

21…伝送用復号器

22…記録部

23, 33…メディア固有鍵生成回路

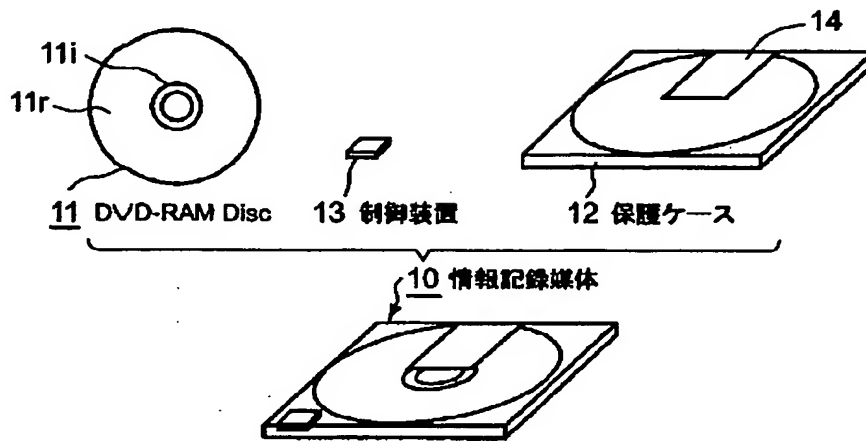
24, 24a, 36, 36a…管理情報処理回路

25…コンテンツ暗号化部

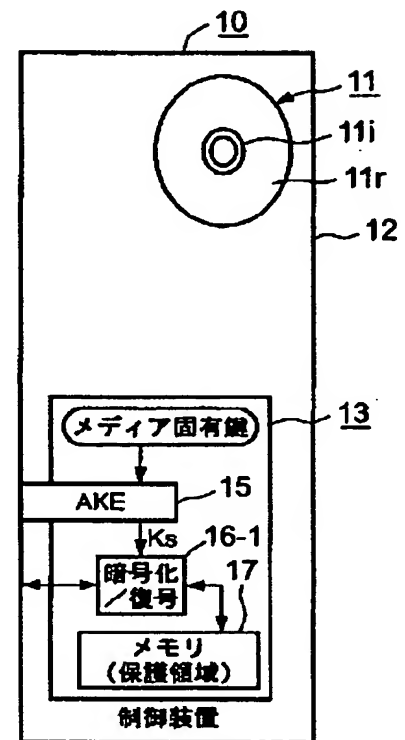
26, 26a...暗号化鍵生成回路
 27, 27a...鍵暗号化部
 30...再生装置
 31...伝送用暗号化器

32...再生部
 37, 37a...復号鍵生成回路
 38, 38a...鍵復号部
 39...コンテンツ復号部

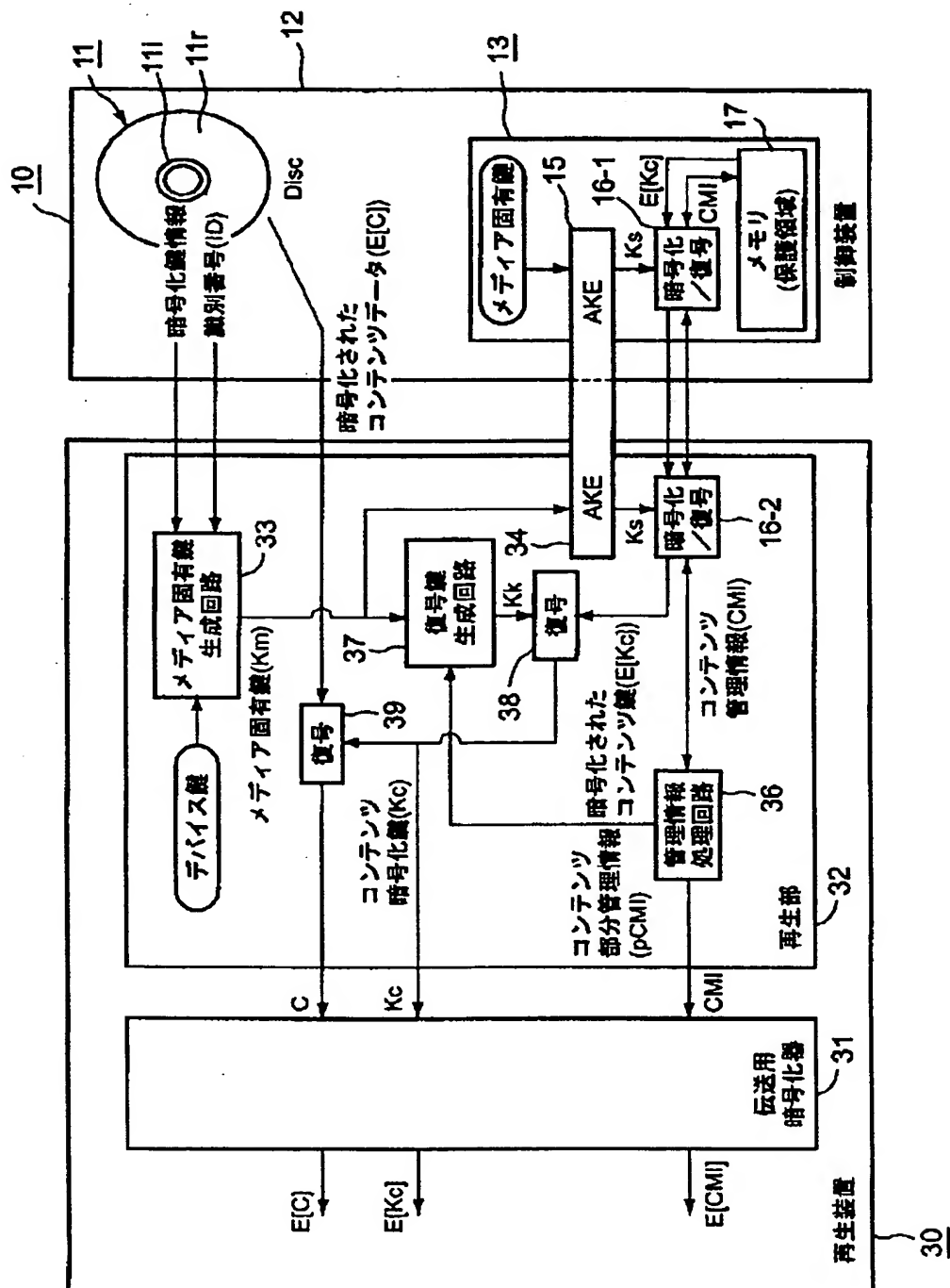
【図1】



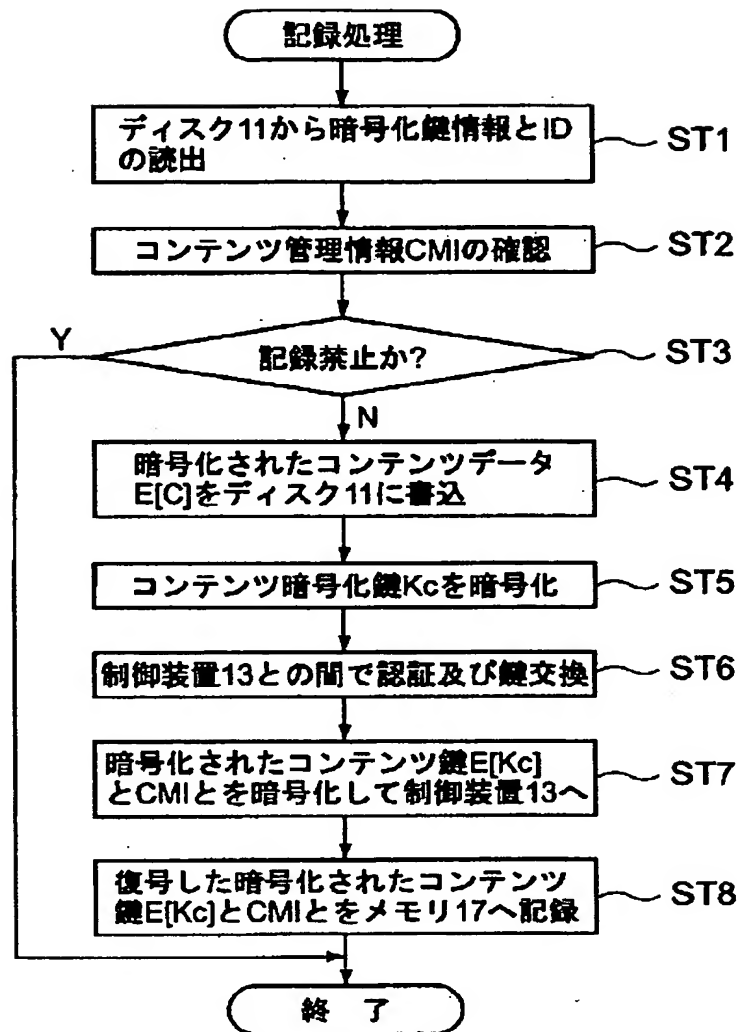
【図2】



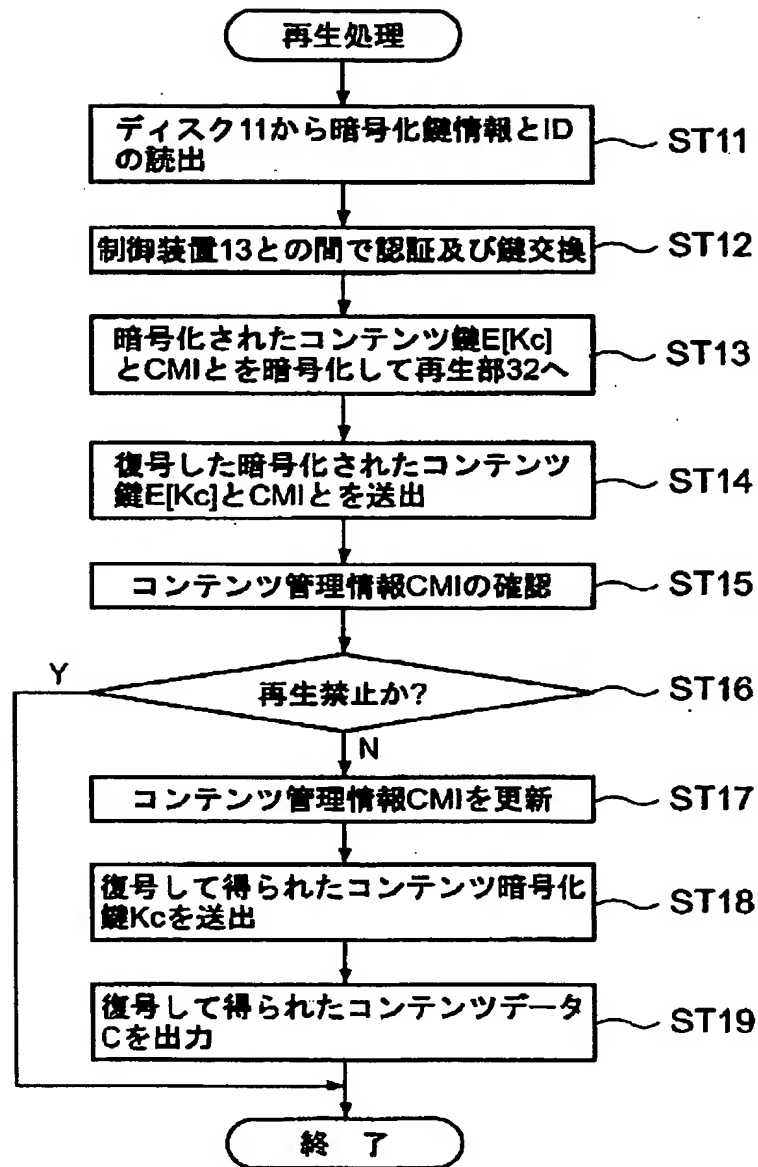
【図4】



【図5】

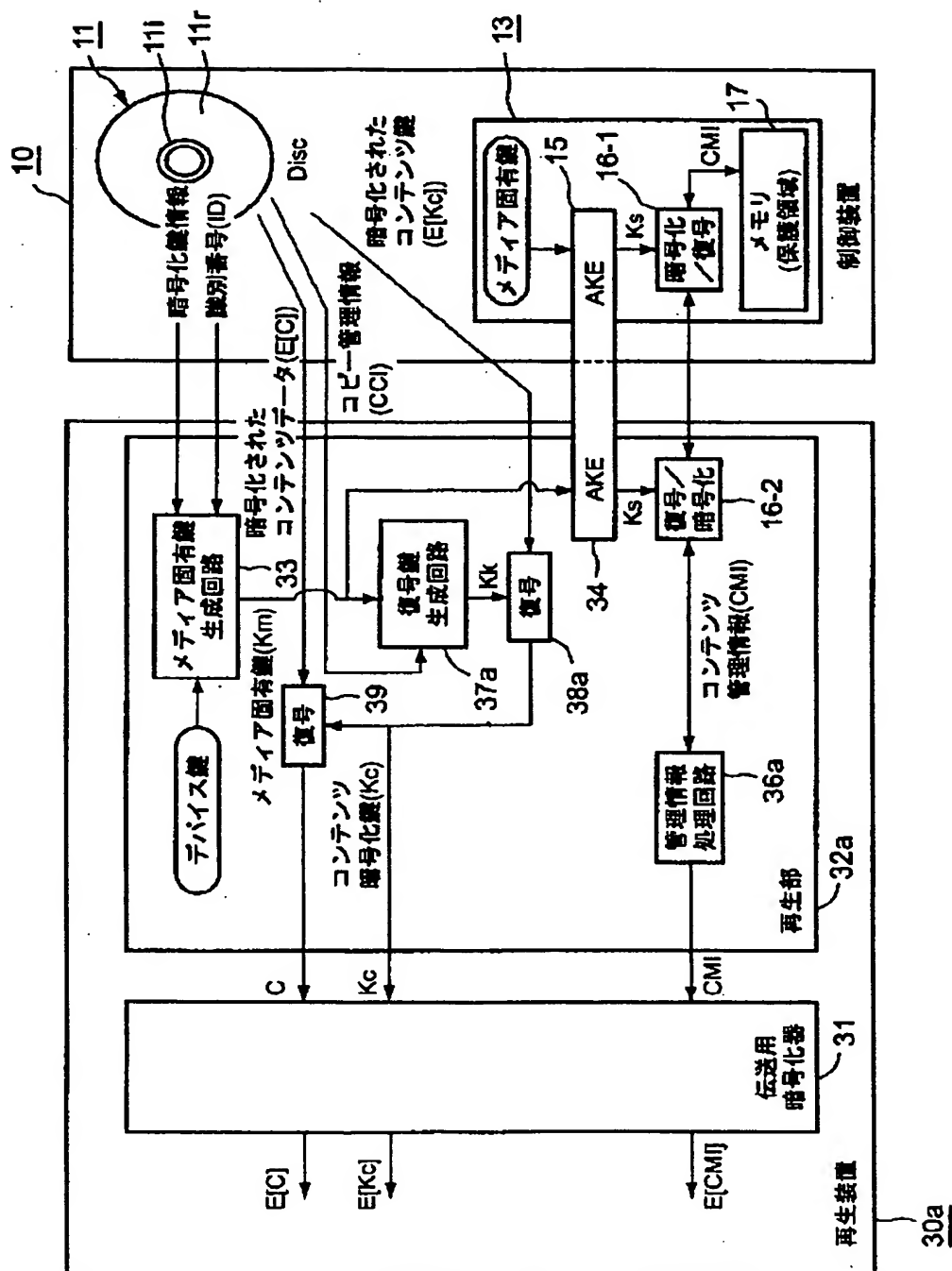


【図6】

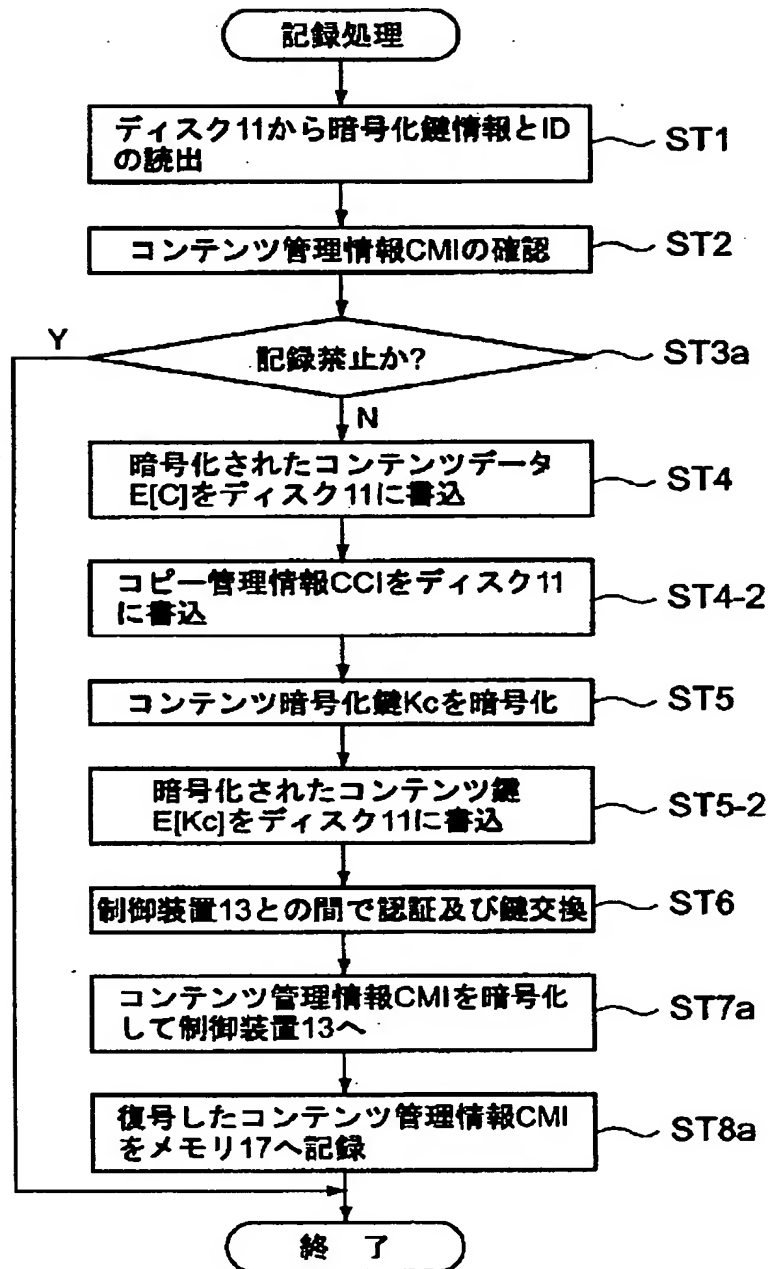


20a

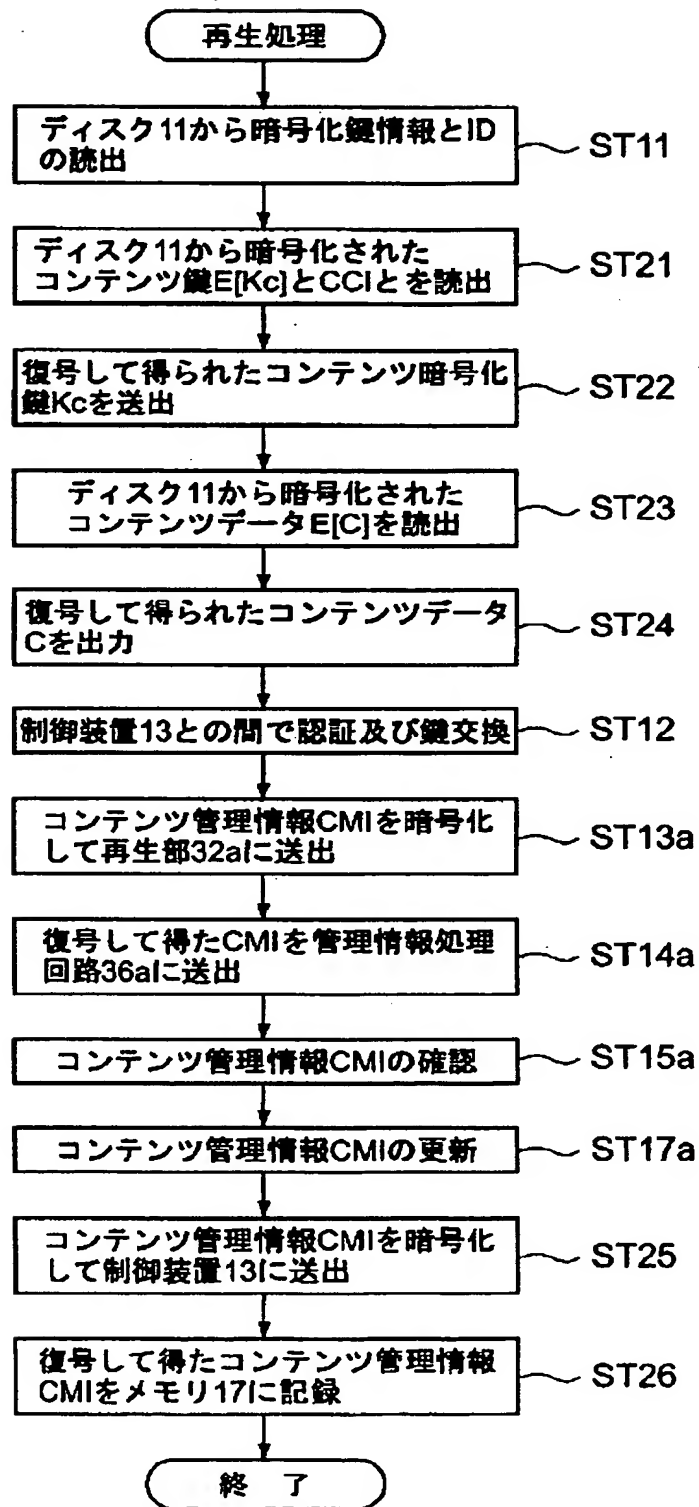
【図8】



【図9】



【図10】



フロントページの続き

(51) Int. Cl. 7

H 0 4 N 5/92

識別記号

F I

H 0 4 N 5/92

メモ (参考)

H